

REMARKS

The Examiner's Answer newly rejected Claims 1, 17 and 18 as being anticipated by U.S. Patent No. 5,029,296 to Marino et al. ("Marino"). Applicants request that prosecution be reopened to permit Applicants to address the new grounds of rejection. Applicants have extensively amended Claims 1, 17 and 18 to more clearly distinguish over the cited references. For at least the reasons explained below, Applicants submit that the present application is in condition for allowance, which action is respectfully requested.

Status of the Claims

Claims 1, 17 and 18 were rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,029,206 to Marino, et al. ("Marino"). Claims 2-8, 10, 11 and 14 were rejected under 35 U.S.C § 103(a) as unpatentable over Marino in view of U.S. Patent No. 6,131,163 to Wiegel ("Wiegel"). Claims 9 and 13 were rejected under 35 U.S.C § 103(a) as unpatentable over Marino in view of U.S. Patent No. 5,845,068 to Winiger ("Winiger"). Claim 12 was rejected under 35 U.S.C § 103(a) as unpatentable over Marino in view of User Manual mod_ssl version 2.6 ("Mod_SSL"). Claim 15 was rejected under 35 U.S.C § 103(a) as unpatentable over Marino in view of U.S. Pre-Grant Publication No. 2002/0116605 to Berg ("Berg"). Claim 16 was rejected under 35 U.S.C § 103(a) as unpatentable over Wiegel in view of T. Dierks et al, "Network Working Group Request For Comments 2246, The TLS Protocol" ("Dierks").

The Claims Are Patentable Over Marino

The Examiner's answer states that in Marino, "the black application software and the receiving application must receive the cryptographic association which contains the security policy information in the form of parameters and uses the cryptographic association to execute their applications in order to decrypt the data." Examiner's Answer, p. 4. Accordingly, the Examiner's answer asserts that Marino provides security policy information usable for more than one executing application program. The Examiner's answer further states that Marino teaches using security parameters for more than one application program, because "the security

parameters are passed by a requesting application program in order to set up a cryptographic association.” Examiner’s Answer, p. 10.

Claim 1, as amended, recites as follows (emphasis added):

1. A method of improving security processing in a computing network, comprising:
 - providing security processing in an operating system kernel;
 - providing first and second application programs which make use of the operating system kernel during execution;
 - providing security policy information that is usable for more than one executing application program;
 - executing the first application program;
 - selectably encrypting at least one remote communication of the executing first application program using the provided security processing in the operating system kernel, under conditions specified by the security policy information;
 - executing the second application program; and
 - selectably encrypting at least one remote communication of the executing second application program using the provided security processing in the operating system kernel, under conditions specified by the security policy information.

Accordingly, Claim 1, as amended, recites selectably encrypting a remote communication of a first application program using security processing provided in the operating system kernel under conditions specified by security policy information, and selectably encrypting a remote communication of a second application program using the provided security processing, also under conditions specified by the security policy information. Such recitations are not taught or suggested by Marino.

Marino discloses a processor architecture including a red processing side 7, a black processing side 8 and a security kernel 6 between the red processing side and the black processing side. See Marino, Fig. 3 and accompanying description. Data on the red processing side can be clear text or encrypted text, but data on the black processing side can only be encrypted (cypher) text. Marino 2:52-57; 9:18-20 ("Further, it is to be noted that only encrypted data exists and is handled by the black side application software). Thus, the black side application programs never handle decrypted data. Thus, in the system of Marino, only red side applications can request encryption/decryption by the security kernel 6. See Marino 9:35-38

("That is, the application program requesting the encrypt or decrypt and the program to receive the encrypted or decrypted data must reside on the red side of the system.") (Emphasis added.)

Accordingly, the security kernel 6 of Marino would not selectably encrypt a communication of a black application program under any circumstances, much less do so under conditions specified by security policy information, as recited in Claim 1.

The black side 8 apparently does assist in the transmission of data to remote systems. For example, for a red application to output data to another system, the data must be encrypted by the security kernel 6 and stored in the black memory for output to the other system. Marino 3:1-3. In order to facilitate a transfer of encrypted data between a red application and a remote system, a cryptographic association is created. However, as noted above, the cryptographic association is not used to encrypt a communication of a black side application program.

As noted by Applicants in the Amendment After Final dated May 16, 2006, in order to establish a secure communication with a remote entity, the system of Marino relies on information provided to the security processing modules by the application programs themselves. See, e.g., Marino 7:36-50. A cryptographic association created in response to a request by a red application program may be subsequently referenced by the application program when a request to encrypt or decrypt data is made. Marino 9:2-5. However, Marino does not provide any teaching or suggestion that one red application would have any awareness of a cryptographic association created by another red application program, or of the information provided by the one red application program to create the cryptographic association. Notably, for example, Marino does not appear to describe re-using a cryptographic association created by one red application for a communication by a second red application. Furthermore, when a cryptographic association is established, Marino states only that "KMUA 40 notifies the **requesting** red side application software 72 of this fact via transfer 108 through red system management application 71." Marino 8:36-39 (emphasis added). Thus, Marino does not teach notifying any red applications of the establishment of the cryptographic association other than the application that requested the cryptographic association.

Accordingly, in the system of Marino, after a first red application program has established a cryptographic association using security information provided by the first red

application program to the security kernel 6, a second red application program desiring to encrypt data for transmission must first establish a new cryptographic association. Thus, the second red application would not use the security information provided by the first application program, but would instead provide its own security information to the security kernel 6. This is in direct contrast with methods according to Claim 1, in which the communications of both the first and second application programs are encrypted using conditions specified by the same provided security policy information.

From the foregoing discussion, it is clear that Marino does not teach or suggest many of the recitations of Claim 1, and Applicants respectfully request that the rejection of Claim 1 as anticipated by Marino be withdrawn. Similar arguments apply to Claims 17 and 18. Accordingly, Applicants submit that Claims 1, 17 and 18 are patentable over Marino.

The Claims are Patentable Over Marino and Wiegel

Applicants' arguments regarding the lack of motivation to combine Marino and Wiegel are incorporated herein by reference but will not be repeated for brevity.

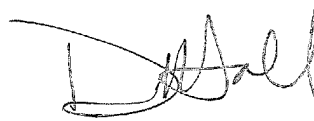
However, Applicants again note that, even if combined, the hypothesized combination of Marino and Wiegel would not teach or suggest each and every recitation of Claims 1, 17 and 18. As noted in the Appeal Brief, even if Marino and Wiegel were combined, it would simply provide the system of Marino with port-level security processing as described in Wiegel, and would not suggest a system that selectably encrypts a communication of an executing application program using provided security processing in the operating system kernel, under conditions specified by security policy information that is usable by more than one application program, as recited in Claim 1. While port level security may be a desirable attribute of a system, it has no relation to selectably encrypting a communication of an executing application program using security processing provided in an operating system kernel, as recited in Claim 1. Similar arguments apply to Claims 17 and 18. Accordingly, Applicants submit that Claims 1, 17 and 18 are patentable over Marino in view of Wiegel.

Dependent Claims 2 and 4-16 are patentable at least as per the patentability of Claim 1.

CONCLUSION

In light of the above amendments and remarks, Applicants respectfully submit that the above-entitled application is in condition for allowance. Favorable reconsideration of this application is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'D. Hall', with a stylized flourish at the end.

David C. Hall
Registration No. 38,904

Customer Number 46589
Myers Bigel Sibley & Sajovec, P.A.
P.O. Box 37428
Raleigh, NC 27627
919-854-1400
919-854-1401 (Fax)